REMARKS/ARGUMENTS

The Examiner rejected claims 1-11 as failing to comply with the enablement requirement (35 U.S.C. §112, par. 1) on the grounds that the claim term "item" and its use in the claims are not described in the Application. (Third Office Action, pg. 2) Applicants traverse.

In particular, the Examiner asked why was the updated item retrieved and built on the user's computer when the user configuration already shows the item as updated and that if an item is updated, does this imply the update is elsewhere? (Third Office Action, pg. 2)

First off, Applicants note that the Application specifically discloses the claim requirements concerning the updating of the application items. For instance, page 12, lines 18-24 and page 14, lines 1-12 of the Application disclose the claim requirements concerning determining whether an application item in the configuration is updated, and if so retrieving the updated item and building the application from the updated item. Applicants submit this disclosure is enabling with respect to the claimed operations performed in that someone skilled in the art reading this disclosure would understand how to implement the claimed operations.

In response to the Examiner's question why was the updated item retrieved and built on the user's computer when the user configuration already shows the item as updated, Applicants submit that the claims do not recite that the user configuration shows the item as updated. Instead, the independent claims recite "determining if the item described in the user configuration has been updated." Applicants submit that the claim requirement of "determining if the item described in the user configuration has been updated" does not specify or require that the user configuration shows that the item is updated, only that such a determination be made. In response to the Examiner's question that if an item is updated, does this imply the update is elsewhere, Applicants respond that the independent claims require "retrieving the updated item if the item has been updated", which implies the item is accessed from some location somewhere.

With respect to the Examiner's objection to the language of "determining if the item described in the user configuration has been updated producing an updated item", Applicants amended the phrase to clarify that the "updated item" comprises the update version of the item that was the subject of the determination.

Accordingly, Applicants submit that the claims comply with the enablement (35 U.S.C. §112, par. 1) and definiteness (35 U.S.C. §112, par. 2) requirements.

The Examiner rejected claims 1, 6, and 11 as obvious (35 U.S.C. §103) over Kenner (U.S. Patent No. 6,314,565) in view of Stedman (U.S. Patent No. 6,262,726). Applicants traverse with respect to the amended claims.

Amended claims 1, 6, and 11 updating an application program for execution by a particular user on a local data processing system, said data processing system comprising the local data processing system and a remote data processing system, and require: defining a user configuration of the application program corresponding to the particular user of the application program at the remote data processing system, the user configuration describing an item from which the application program may be built; determining that the user configuration corresponds to the particular user; downloading the user configuration to the local data processing system in response to determining that the user configuration corresponds to the particular user; determining if the item described in the user configuration has been updated with an updated item; retrieving the updated item if the item has been updated; and building the application program with the updated item.

Applicants amended claims 1, 6, and 11 to require that the user configuration is at the remote data processing system, downloading the user configuration to the local data processing system in response to determining that the user configuration corresponds to the particular user, and that the determination is made if the item is updated "with" an updated item.

Applicants submit that the following combination of requirements is nowhere shown in the cited art: defining a user configuration of the application program corresponding to the particular user of the application program at the remote data processing system, where the user configuration describes an item from which the application program may be built; downloading the user configuration to the local data processing system; determining if the item described in the user configuration has been updated with an updated item and then retrieving the updated item and building the application program with the updated item.

For instance, the cited col. 7, lines 5-16 of Kenner (Third Office Action, pg. 3) discusses how a user system registry is queried to identify installed codecs by comparing codecs in the downloaded script file with codecs indicated in the registry. The cited col. 8, lines 18-41 (Third Office Action, pg. 3) then mentions that a codec is downloaded and installed according to the instructions in the script file.

The Examiner recognized that the cited Kenner does not teach the claimed user configuration corresponding to the particular user. Applicants further note that Kenner also does not teach the claim requirement that the defined user configuration for the particular user is at the remote data processing system. Instead, in the cited Kenner, the script file is downloaded from the remote server, but as the Examiner recognizes, the script file of Kenner is not for a particular user. Nor does the cited Kenner disclose the claim requirements concerning downloading the user configuration to the local data processing and using the downloaded user configuration to determine if an item described in the user configuration has been updated.

The Examiner cited col. 6, lines 55-62 of Stedman as teaching additional of these claim requirements not taught in Kenner. (Third Office Action, pgs. 3-4) Applicants traverse.

The cited col. 6 of Stedman discusses how a user must enter a user name and password and that the configuration files of the operating system keeps track of a particular user. Nowhere in the cited Stedman is there any teaching, suggestion or mention of the claim requirements of a user configuration at a remote system that is downloaded, and that a determination is made of the user configuration to determine if an item is updated, and if so retrieving the updated item and building the application with the updated item.

Moreover, Applicants submit that the combination of Stedman and Kenner also nowhere teach or suggest the above requirements, alone or in combination.

Certain of the dependent claims, such as claim 3, include requirements of downloading a file from the remote server. The amended independent claims now require downloading the user configuration. The Examiner referenced the rejection in the Second Office Action dated October 27, 2003, in which the Examiner cited col. 22, lines 55-59 of Hayes (U.S. Patent No 6,205,476)

as teaching the requirements concerning downloading from a remote server. (Third Office Action, pg. 5)

The cited col. 22 of Hayes mentions storing the configuration preferences for the end user on the server and downloading a set of preferences stored for a given context to a workstation when requested by a user.

Although the cited Hayes mentions storing configuration preferences on a server and downloading to a workstation, nowhere does the cited Hayes anywhere teach the claim requirement of downloading a user configuration to a local data processing system and then determining if an item described in the user configuration has been updated, and if so retrieve the updated item and build the application program with the updated item. Applicants further submit that neither Kenner nor Stedman teach or suggest the claim requirements concerning using a downloaded configuration to determine if an item described in the user configuration was updated and if so retrieving and using to build the application program.

Accordingly, claims 1, 6, and 11 are patentable over the cited art, because the cited art in combination and alone does not teach or suggest the combination of claim requirements.

Claims 2-5, 7-10, and 12-14 are patentable over the cited art because they depend from one of claims 1, 6, and 11. The following dependent claims provide additional grounds of patentability over the cited art.

Claims 2, 7, and 12 depend from claims 1, 6, and 11 and further require encrypting and storing the user configuration in a manifest file, wherein the user configuration is downloaded to the local data processing system in the manifest file, and wherein determining that the user configuration corresponds to the particular user comprises authenticating the particular user in response to the particular user requesting the application program; and decrypting the manifest file to produce a decrypted user configuration in response to the user authentication, wherein the decrypted user configuration is used to determine if the item described in the user configuration has been updated.

Applicants amended these claims to clarify the relationship with the base claims and remove limitations redundant with those in the base claims.

The Examiner referenced the rejection in the Second Office Action dated October 27, 2003, in which the Examiner cited col. 1, lines 13-21 of Hsu (U.S. Patent No. 5,894,515) as teaching the claim requirements concerning encrypting and decrypting the manifest file. (Third Office Action, pg. 5) Applicants traverse and submit that the cited art does not teach or suggest the claimed combination.

The cited col. 1 of Hsu discusses encryption and decryption in general and the use of encryption to protect data from an unauthorized user. Nowhere does the cited Hsu anywhere teach or suggest storing the user configuration in a manifest file and then decrypting the manifest file to produce a decrypted user configuration that is used to determine whether the item described in the user configuration has been updated.

Further, nowhere does the cited Kenner and Stedman teach storing the user configuration in a manifest file that is decrypted in response to user authentication to determine whether the item described in the user configuration has been updated.. The cited col. 7, lines 8-12 and 17-32 of Kenner (Second Office Action, pg. 6) discusses how a registry file is queried to identify installed codecs and their verison, where applications post and retrieve registry information to determine or alter system and software configuration data. Further, the cited col. 7 mentions that the stored codec information does not need to be in the system registry, and that this information may be updated when the codecs are installed.

Nowhere in the cited col. 7 of Kenner is there any teaching or suggestion of storing the user configuration in a manifest file and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used to determine whether the item described in the user configuration has been updated.. There is no mention in the cited col. 7 of storing user configuration information or the registry file in a manifest that is decrypted in response to user authentication and used to determine whether the item described in the user configuration has been updated so the updated item may be retrieved and used to build the application.

The cited col. 6, lines 58-62 of Stedman (Second Office Action, pg. 6) mentions that to initialize the operating system, the user must enter his or her username and password, and that configuration files keep track of the user, and the desktop layout for the user.

The cited Kenner discusses how a registry file is queried to determine codecs to install and Stedman discusses user authentication. However, nowhere in the cited combination of Kenner and Stedman is there any teaching or suggestion of the claim requirement of storing the user configuration in a manifest file and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used to determine if the item described in the user configuration has been updated.

Moreover, even if one were to modify the systems of Kenner and Stedman with Hsu to provide encryption, the proposed modification still does not teach the claim requirements. For instance, modifying the cited Kenner with encryption would provide an encrypted registry file having information used to install a codec. Modifying the cited Stedman with encryption would provide some encrypted authentication. All the combination of references still nowhere teach or suggest the sequence of claim requirements of storing the user configuration in a manifest file, which is encrypted, and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used to determine if the item described in the user configuration has been updated so that the updated item may then be retrieved and used to build the application program.

Accordingly, claims 2, 7, and 12 provide additional grounds of patentability over the cited art because the additional requirements of these claims are not taught or suggested in the cited art.

Claims 3, 8, and 13 include many of the additional requirements of claims 2, 7, and 12 and thus provide additional grounds of patentability for the reasons discussed with respect to claims 2, 7, and 12.

Claims 4, 9, and 14 depend from claims 3, 8, and 13 and further require downloading data from the remote data processing system to the local data processing system according to the decrypted user configuration.

In the referenced Second Office Action, the Examiner cited col. 7, lines 12-16 and col. 8, lines 18-29 of Kenner and col. 6, lines 58-62 of Stedman as teaching the additional requirements of these claims. (Second Office Action, pg. 7). Applicants traverse.

The cited col. 7 mentions that the codec information in the script file is compared to that in the registry to determine a list of newly available and uninstalled codecs. The cited col. 8 mentions providing a codec provider with information needed to download the files. The cited col. 6 of Stedman mentions a user entering a username and password to initialize the operating system.

The cited Kenner does not teach or suggest the claim requirement of downloading data from a remote system according to a decrypted user configuration. Instead, the cited Kenner determines codecs to download based on new codecs indicated in a script file and the user registry. Nowhere does Kenner anywhere teach or suggest that the registry file used to download data was itself downloaded from the remote server.

Stedman discusses a user entering a password to initialize the operating system. Nowhere does the cited Stedman anywhere teach or suggest decrypting a downloaded user configuration that is used to download data too.

Moreover, nowhere do the cited Kenner and Stedman anywhere teach or suggest downloading the data according to the decrypted user configuration in addition to downloading an updated item, as required by the base claims.

Accordingly, claims 4, 9, and 14 provide additional grounds of patentability over the cited art because the additional requirements of these claims are not taught or suggested in the cited art.

Claims 5, 10, and 15 depend from claims 4, 9, and 14 and further require authenticating the particular user in response to the particular user requesting the application program, wherein the data is downloaded from the remote data processing system in response to the user authentication.

Applicants amended claims 5, 10, and 15 to clarify the relationship with the base claims.

The Examiner cited the same sections of Kenner and Stedman cited with respect to claims 4, 9, and 14 as teaching the additional requirements of these claims.

Applicants submit that the cited Kenner and Stedman nowhere teach or suggest authenticating a particular user in response to the user requesting an application and downloading data according to a stored user configuration that was previously decrypted and used to determine if updated items need to be retrieved, per the requirements in the intervening claims 3, 8, and 13.

Accordingly, claims 5, 10, and 15 provide additional grounds of patentability over the cited art because the additional requirements of these claims are not taught or suggested in the cited art.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-15 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0460.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: July 16, 2004

By: _____
David W. Victor
Registration No. 39,867

Please direct all correspondences to:
David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984